Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc. and Non-Prioritized Defendants Mark Zuckerberg and Sheryl Sandberg

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

REPLY IN SUPPORT OF MOTION OF DEFENDANT FACEBOOK, INC. TO DISMISS PLAINTIFFS' CONSOLIDATED COMPLAINT

Judge: Hon. Vince Chhabria
Courtroom 4, 17th Floor
Hearing Date: January 23, 2019
Hearing Time: 10:30 a.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUHTORITIES

Page(s)

TABLE OF AUTHORITES

Page(s)

TABLE OF AUTHORITIES

I. INTRODUCTION

Plaintiffs' opposition brief confirms that they lack Article III standing. The only thing the named Plaintiffs appear to have in common is that they received a notice from Facebook informing them that Dr. Kogan may have improperly shared some of their data with Cambridge Analytica, in violation of Facebook's policies. Opp. at 5. Plaintiffs admit that the information possibly shared with Cambridge Analytica did not include social security numbers, credit card numbers, passwords, or other types of data at issue in "typical 'data breach' cases" where the threat of identity theft may give rise to standing. *Id*. at 5. Plaintiffs claim they have "already been victim" of "phishing attempts, attempts to gain unauthorized access to their Facebook accounts, and Facebook friend requests from impostor accounts," *id.* at 6, but make no effort to link these occurrences to Kogan or Cambridge Analytica. In the end, Plaintiffs retreat to generic and vague concerns about "offensive privacy violations" and their dislike of "unwanted, outrageous targeted political and sales marketing." Opp. at 7. No court has ever found Article III standing based on such non-specific, non-concrete, non-particularized harm. This Court should not be the first.

Standing is not the only barrier to relief; the Court also should dismiss this case because Plaintiffs consented to the alleged conduct at issue. As Facebook's moving brief demonstrated, the operative complaint contains binding admissions that mandate dismissal of this action. The complaint admits, for example, that Plaintiffs assented to Facebook's Terms of Service and its Statement of Rights and Responsibilities. Compl. ¶ 527. It admits that "Facebook provided 'Privacy Settings' to users, and made them prominent and accessible." *Id.* ¶ 9. It admits that apps could obtain user data only "[a]s long as the request complies with the user's and/or friends' privacy settings." *Id*. ¶¶ 121-122. And it admits that "[t]here is nothing wrong with targeted advertising." *Id*. ¶ 110.

Recognizing that these allegations plead them out of court, Plaintiffs' opposition brief attempts to disavow each of these fatal admissions. Plaintiffs now say they never assented to any contract at all. Opp. at 10. They assert that Facebook's privacy settings were "illusory," and that users were *not* told "clearly and prominently" that their data could be shared with apps by their friends. *Id*. at 1-2. And they proclaim that advertising techniques "target[ing] users with political and other content" are "unscrupulous" and "harmful and invasive." *Id*. at 3-4.

The reason for this about-face is clear: the factual allegations Plaintiffs included in the Complaint

end this case as a matter of law. But Plaintiffs cannot avoid the implications of their own admissions by trying to recharacterize them in their briefing. The Complaint and the documents incorporated therein leave no doubt that Plaintiffs consented to the very practices about which they now complain, including the sharing of their data with third-party apps and device manufacturers and the receipt of targeted advertising. Indeed, just this month, the Ninth Circuit agreed with this conclusion, upholding a district court ruling that Facebook users consented to some of the very same policies at issue here. *Smith v. Facebook, Inc.*, 2018 WL 6432974, at *1 (9th Cir. Dec. 6, 2018). As the Ninth Circuit explained, "[a] reasonable person viewing those disclosures would understand that Facebook maintains the practices of (a) collecting its users' data … and (b) later using the data for advertising purposes." *Id.*

In short, despite ample opportunity and the benefit of substantial pre-complaint discovery, Plaintiffs have failed to identify any viable theory of Article III injury or any viable cause of action. The Court should dismiss this case with prejudice.

II. ARGUMENT

A. Plaintiffs Lack Article III Standing

Plaintiffs' brief identifies three theories of injury: (1) "a substantial threat of identity theft or fraud," (2) "a cognizable injury to their privacy interests," and (3) "injury to their property interests." Opp. at 5-10. Plaintiffs' own arguments confirm that each of these theories fails.

1. ***Plaintiffs are not at imminent risk of identity theft.*** As Facebook explained, the data users shared with apps through Facebook bears no resemblance to the kinds of data courts have held may give rise to an actionable risk of identity theft. MTD at 17-18. Plaintiffs do not dispute that their theory of injury is unprecedented when they recognize that "'no court has ever accepted' the[ir] theory 'of identity theft.'" Opp. at 6. But they proclaim "[t]he scope of the information" involved in this case "is far beyond that addressed in typical 'data breach' cases." Opp. at 5. Plaintiffs' own Complaint belies this assertion, acknowledging that the thisisyourdigitallife app could access only limited categories of information: users' "*Public* Facebook Profile, including their name and gender; Birth date; Current city if the friends had chosen to add this information to their profile; Photographs in which the friends were tagged; and Pages that the friends had liked." Compl. ¶ 147 (emphasis added). Plaintiffs speculate that *other* categories of information belonging to some *other* unnamed users might have been disclosed to *other* apps, but that

cannot establish standing on behalf of the named plaintiffs. *Lewis v. Casey*, 518 U.S. 343, 357 (1996).

Nor can Plaintiffs establish standing by asserting that the "52,000 unique data points" Facebook allegedly collects are of the type "commonly used for identity theft and fraud." Opp. at 5. Plaintiffs do not explain what these data points are, with which apps they allegedly were shared, how they are tied to the named Plaintiffs, or whether any named plaintiffs even set them to be non-public. Indeed, Plaintiffs concede that their Complaint says *nothing* about their own privacy settings. Opp. at 23. Plaintiffs further contend (without any basis) that "Russian and other foreign and domestic operatives now possess users' content and information, including private messages, photos and posts"—but, again, there is no allegation that these unspecified "operatives" obtained *Plaintiffs'* data, or that they obtained such data to steal identities. Opp. at 5-6. Rather, Cambridge Analytica allegedly obtained user data to inform targeted ad campaigns, not to engage in identity theft. Compl. ¶¶ 5, 135, 144, 386, 538.

Also not tied to Facebook's conduct is the claim that four named plaintiffs experienced "phishing attempts, efforts by hackers trying to access or log in to their Facebook accounts, friend requests from trolls or cloned or imposter accounts, or other interference with their Facebook accounts." Compl. ¶ 408. Plaintiffs rely on a mention of "phishing" in *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018), but there the Ninth Circuit held that the exposure of "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information" gave "hackers the means to commit fraud or identity theft." *Id.* at 1023, 1027. This case is markedly different. Plaintiffs identify no specific content they shared, and admit that the information giving rise to standing in *Zappos* is *not* at issue here. Compl. ¶ 12.

Plaintiffs also argue that they "have paid for credit monitoring and incurred time and out-of-pocket costs to protect themselves" from identity theft. Opp. at 6. But a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011). "Mitigation expenses do not qualify as actual injuries where the harm is not imminent." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015). And there is certainly no imminent harm here, as Cambridge Analytica allegedly received this information more than 3 years ago.

2. ***Plaintiffs have not suffered any cognizable privacy injury***. Plaintiffs say they have standing

because (1) the disclosure of their information "damaged" their privacy interests and (2) they were "subject to psychographic marketing." Opp. at 7-8. Again, this is not enough. Merely labeling such activities a "privacy injury" does not establish standing. *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (disclosures "without any concrete consequences" do not give rise to Article III injury); *Nayab v. Capital One Bank, N.A.*, 2017 WL 2721982, at *2–3 (S.D. Cal. June 23, 2017) (similar); *In re Google, Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012). As discussed below, pp. 13-18, Plaintiffs' invasion-of-privacy allegations bear no resemblance to common-law privacy torts. And Plaintiffs still offer no explanation of how receiving "targeted political and sales marketing" from an independent third party, Opp. at 7, implicates any common-law privacy interest.

3. ***Plaintiffs have not suffered any economic loss***. Plaintiffs argue that their "content and information has value" because it "generated billions of dollars in revenue for Facebook" (Opp. at 8), but "injury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal identification information." *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013). "[I]njury in fact cannot be based solely on a defendant's gain; it must be based on a plaintiff's loss." *Silha v. ACT, Inc.*, 807 F.3d 169, 174–75 (7th Cir. 2015). The value of "demographic information" does not "constitute[] damage to consumers or unjust enrichment to collectors." *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012).

Plaintiffs also fail to allege a *market* for their personal information, necessary for any theory that the value of their personal information was diminished. They contend they need only "'allege that there was either an economic market or that it would be harder to sell their own PII, not both.'" Opp. at 10 (quoting *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) ("*Anthem II*")). But Plaintiffs cannot allege that it is more difficult to sell their PII without alleging that there was someone willing to buy it. *See In re Google, Inc. Privacy Policy Litig.*, 2015 WL 4317479, at *5 (N.D. Cal. July 15, 2015); *Chambliss v. Carefirst, Inc*, 189 F. Supp. 3d 564, 572 (D. Md. 2016). Here, Plaintiffs identify only a black market for "online identit[ies], including hacked financial accounts" and "Facebook logins" (Compl. ¶ 409)—not one for consumers to sell the type of (largely public) information allegedly disclosed here.

Even if Plaintiffs could allege the existence of a market, they cannot allege that Facebook made

it harder to sell their information or diminished its value. *See In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 932 (N.D. Cal. 2015) (allegation of market for browsing histories did not establish an injury-in-fact where plaintiffs did "not also allege[] an inability to participate in these programs after Facebook collected their information"). Plaintiffs do not argue that they were "foreclosed from entering into a 'value-for-value exchange.'" *Low v. LinkedIn Corp.*, 2011 WL 5509848, at *4-5 (N.D. Cal. Nov. 11, 2011); *In re iPhone Application Litig.*, 2011 WL 4403963, at *4 (N.D. Cal. Sept. 20, 2011). Instead, they argue only that the value of their information was somehow diminished because Facebook made it "ubiquitously available." Opp. at 8. But the Complaint pleads no facts supporting this allegation: Plaintiffs allege their information was obtained by a single app, not disseminated through broad public disclosure, and they do not allege the data was made available on any market. Rather, the only alleged use was to target ads to users. *See, e.g.,* Compl. ¶ 22. This limited use of Plaintiffs' information did not diminish its value.

* * *

At bottom, Plaintiffs do not plausibly allege that they, personally, have suffered any concrete or particularized injury whatsoever. The case law is clear that the mere targeting of ads—using limited information that Plaintiffs voluntarily shared with their Facebook friends and/or made available directly to apps, and *not* including sensitive financial information like social security numbers, credit card numbers, or passwords—cannot constitute a "privacy" injury. *See, e.g.*, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) (holding that a plaintiff must allege facts showing a specific, personal harm and instructing courts to consider whether that harm "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit"); *cf. Zappos.com*, 888 F.3d at 1023 (finding standing where hackers stole "account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information"). For that reason alone, the Court should dismiss this case.

B. Plaintiffs Consented To All Of The Challenged Practices

Plaintiffs try to run away from their own allegation that they consented to Facebook's Terms of Use. Compl. ¶ 527; MTD at 24. They now argue that they did not form a contract with Facebook when they registered for an account because "[t]he existence of references to the Terms of Use and Privacy

Policy were not reasonably conspicuous." Opp. at 11. Not only is this argument contrary to Plaintiffs' own pleading, but multiple courts also have rejected it. *See, e.g.*, *In re Facebook Biometric Information Privacy Litig.*, 185 F. Supp. 3d 1155, 1166-67 (N.D. Cal. 2016); *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 835-41 (S.D.N.Y. 2012); *E.K.D. ex rel. Dawes v. Facebook, Inc.*, 885 F. Supp. 2d 894, 901 (S.D. Ill. 2012). And for good reason: the law is clear that, by agreeing to the SRR when they registered for Facebook accounts, and by later using their accounts, Plaintiffs consented to Facebook's terms.

Moreover, by consenting to the SRR, Plaintiffs necessarily consented to the Data Use Policy that is specifically identified in the signup process and the SRR itself. The law "presumes that everyone who signs a contract has read it thoroughly." *Roldan v. Callahan & Blaine*, 219 Cal. App. 4th 87, 93 (2013). As Plaintiffs concede, "the SRR said that the Data Use Policies were intended 'to make important disclosures'" about how Facebook uses their information, and Plaintiffs do not dispute that the SRR "encourage[d] [them] to read the Privacy Policy, and to use it to help make informed decisions." Opp. at 13.

In light of these undisputed facts and binding admissions, Plaintiffs' argument that "[r]easonable readers did not know that the offer to contract included the Data Use or Privacy Policies" (Opp. at 13) is wrong as a matter of law. The SRR informs users that Facebook's use of their data is governed by Facebook policies: Facebook "designed [its] Privacy Policy … to make important disclosures about how [Facebook] collect[s] and can use your content and information." Compl. ¶ 243. Facebook expressly informed users that the Privacy Policy (and later the Data Use Policy) governed "how [Facebook] collect[s] and can use your content and information." *Id.* ¶¶ 243–44.

Plaintiffs try to distinguish *Shaw v. Regents*, 58 Cal. App. 4th 44 (1997), and *Wolschlager v. Fidelity Nat'l Title Ins. Co.*, 111 Cal. App. 4th 784 (2003), on the basis that "[t]he contracts in both of those cases alerted readers that they were consenting to terms contained in other documents." Opp. at 13. But that is exactly what the SRR did—it said that the Data Use Policy "disclos[ed]" how Facebook could "collect and … use [their] content and information." By the plain terms of the parties' agreement, Plaintiffs' use of Facebook, and Facebook's use of their information, was subject to terms in the hyperlinked privacy policy. Having elected to use Facebook, Plaintiffs cannot now claim that they did not consent to its policies. *See* Cal. Civ. Code § 3521 ("He who takes the benefit must bear the burden.").

Indeed, one of Plaintiffs' lead cases, *Anthem II*, 2016 WL 3029783, applied incorporation by

reference under similar circumstances and rejected many of the Plaintiffs' arguments here. There, the court applied *Shaw* and *Wolschlager* to hold that Anthem's insurance policies incorporated its privacy policies. As here, the contract "made clear and unequivocal references to Anthem's privacy policies." *Id*. at *9. These "references were called to the attention of" the insured because "each governing contract … gave instructions on how consumers could review those policies in greater detail." *Id*. at *10. The policies were "easily available," "either via a physical copy or online." *Id*. The *Anthem II* court found that "[t]he references at issue … in fact [went] several steps further than the references in *Wolschlager*," where "plaintiff was simply advised that '[c]opies of the [insurance] policy... should be read,' without making *any* reference to the arbitration clause that was later disputed." *Id*. In *Anthem II*, as here, "the governing documents all discussed [the company's] obligation to protect privacy." *Id*. This case is even clearer than *Anthem II*, as the Data Use Policy was even more readily available: Plaintiffs were shown a hyperlink directing them to the Data Use Policy, whereas the *Anthem II* Plaintiffs had to "either call[] Anthem's customer service department or … visit[] [its] website" to view the full policies. *Id*.

Like the plaintiffs in *Anthem II*, Plaintiffs rely on *Amtower v. Photon Dynamics, Inc.*, 158 Cal. App. 4th 1582 (2008). But just as the *Anthem II* court held, Plaintiffs' "reliance upon *Amtower* is misguided" because "*Amtower* involved two separate contracts governing two different sets of parties." 2016 WL 3029783, at *10. The defendant in *Amtower* sought attorneys' fees under a contract the plaintiff never signed, arguing that an agreement with the plaintiff incorporated the separate fees provision merely by mentioning it. The court disagreed: "unlike the facts in either *Shaw* or *Wolschlager*," the allegedly incorporated agreement was "a separate contract" to which the plaintiff was not a party. *Amtower*, 158 Cal. App. 4th at 1609.

As a last resort, Plaintiffs retreat to the canon that any ambiguities regarding incorporation must be construed against Facebook. Opp. at 14. But this rule applies only to ambiguous contracts, *Victoria v. Sup. Ct.*, 40 Cal. 3d 734, 739 (1985), and here the SRR unambiguously incorporates the Data Use Policy. By contrast, in the case on which Plaintiffs rely, *Chan v. Drexel Burnham Lambert, Inc.*, 178 Cal. App. 3d 632, 643 (1986), the contract did not even mention the purportedly incorporated document.

C. Facebook's Policies Disclosed The Precise Practices At Issue

1. ***Consent may be resolved as a matter of law.*** Because Facebook has shown that multiple

contractual terms establish consent to the precise conduct at issue, Plaintiffs now claim that consent may not be resolved as a matter of law. Opp. at 16. The law is to the contrary. Indeed, the Ninth Circuit confirmed just this month that consent is an objective question that can be resolved on a motion to dismiss in a decision addressing the same Facebook policies at issue here. *Smith*, 2018 WL 6432974, at *1. There, the district court held that plaintiffs consented to Facebook's data tracking and collection practices, and the Ninth Circuit agreed. "In determining consent, courts consider whether the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization." *Id*. The issue may be resolved on a motion to dismiss where "[a] reasonable person viewing [Facebook's] disclosures would understand that Facebook maintains the practices" plaintiffs challenge. *Id*. That is the case here.

2. ***Facebook told users that their friends could share their information with apps.*** Plaintiffs argue that they did not know third parties could access their information from their friends. Opp. at 14. But this argument is belied by clear statements in Facebook's Data Use Policy. As the Complaint admits, the Data Use Policy told users that the information shared with friends could be disclosed to the apps their friends use, Compl. ¶ 275, unless they set their application settings to prevent such sharing. "Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use." *Id.* Plaintiffs admit that the Data Use Policy even provided a concrete example of how this worked: "Your friend might … want to share the music you 'like' on Facebook" with "a music application." *Id*. "If you have made that information public, then the application can access it just like anyone else. But if you've shared your likes with just your friends, the application could ask your friend for permission to share them." *Id*. Plaintiffs admit that the thisisyourdigitallife app allegedly obtained their information through precisely this process. As the graphic on Page 54 of the Complaint states, "[t]he app requested permission from its users, including people who took the test, to access th[e] information about their Facebook friends."

Plaintiffs do not even try to explain why this alleged sharing was not squarely authorized by the language they quote in their Complaint. Rather, they insist that a snippet of this language—"if you've shared your likes with just your friends, the application could ask your friend for permission to share

them"—was insufficient to convey "that app developers would have full access to all of the[ir] content and information." Opp. at 15. But the Complaint does not allege that any app had "full access to all of the[ir] content and information." Rather, it asserts that a single app accessed discrete categories of content, many of which were publicly available. Compl. ¶¶ 146-147. More fundamentally, Plaintiffs ignore the crucial language from the passage quoted at paragraph 275: "if you share something on Facebook, anyone who can see it can share it with … the games, applications, and websites they use." Even if Plaintiffs had alleged that different categories of information were shared with some other third-party app—and their Complaint does not so allege—the language of the Data Use Policy broadly encompassed "all of the content and information" Plaintiffs shared with their friends.

3. ***Facebook told users that service providers could access users' content and information in the course of providing services to Facebook users.*** Plaintiffs argue that Facebook did not "clearly and prominently disclose[]" that it purportedly "allowed its business partners to download users' content and information if third parties engaged with them." Opp. at 14. But the relevant disclosure in Facebook's Data Use Policy encompassed this practice and more, stating "[w]e give your information to the people and companies that help us provide the services we offer" and "partners must agree to only use your information consistent with the agreement we enter into with them, as well as this privacy policy [or 'Data Use Policy']." Compl. ¶¶ 281–84. Plaintiffs do not deny that Facebook required its partners to abide by the Data Use Policy, and nowhere allege that any business partner misused any data, much less data of the named plaintiffs. On the contrary, Plaintiffs admit that these companies said they "did not collect or mine the Facebook data of [their] customers. " *Id.* ¶ 171. Indeed, Plaintiffs do not allege that *any* third party other than the thisisyourdigitallife app obtained their data.

Plaintiffs attempt to characterize Facebook's partnerships as nefarious, but the Complaint itself explains why it was necessary (and consistent with Facebook's user agreements) to share users' information with service providers. Such sharing enabled users to access Facebook "not only on desktop computers, but also on users' mobile phones, smart TVs, game consoles, and other devices." *Id.* ¶ 170. Facebook "allowed manufacturers to integrate 'like' buttons, photo sharing, and friend lists into their devices," *id.*, so that people could "access … their Facebook network and messages" on mobile devices manufactured by companies like Blackberry. *Id.* ¶ 171. Given this context, it is entirely unsurprising

that these devices were able to "retrieve Facebook users' … data." *Id.* ¶ 173.

D. The SRR disclaims liability for third-party conduct

Plaintiffs do not appear to contest that the SRR's exculpatory clause encompasses claims against Facebook based on "the actions … of third parties." *See* Opp. at 18.[1] Instead, they argue that the clause does not apply because "[t]he conduct at the heart of Plaintiffs' complaint … is Facebook's, not that of third parties." Opp. at 18. But the only conduct alleged to have affected Plaintiffs themselves was performed by Cambridge Analytica, which allegedly created harmful advertising, *e.g.*, Compl. ¶ 387, and Kogan, who allegedly gave Plaintiffs' data to Cambridge Analytica, *id.* ¶ 138.

Plaintiffs contend that the exculpatory clause in the SRR is invalid under the "public interest" rule announced in *Tunkl v. Regents of the University of California*, 60 Cal. 2d 92, 101 (1963). But Facebook's services are not "essential," and therefore do not fall within *Tunkl*'s ambit. At issue in *Tunkl* was a release a hospital presented to patients absolving it of liability for negligence as a "[c]ondition[ ] of admission." 60 Cal. 2d at 94. After noting the "obvious[]" premise that "no public policy opposes private, voluntary transactions in which one party, for a consideration, agrees to shoulder a risk which the law would otherwise have placed upon the other party," *id.* at 101, the Court held that certain relationships, by their very nature, are not "voluntary" in that sense. It reasoned that a patient seeking treatment "does not really acquiesce voluntarily in the contractual shifting of the risk, nor can we be reasonably certain that he receives an adequate consideration for the transfer." Rather, "[s]ince the service is one which each member of the public, presently or potentially, may find essential to him, he faces, despite his economic inability to do so, the prospect of a compulsory assumption of the risk of another's negligence." *Id.*

This case is entirely different. No person is compelled to use Facebook—a free social networking service—and those who do use it are not compelled to engage in any particular activity. Users may "coordinate daily activities, network, engage in political and cultural discourse, and pursue interests and hobbies" (Compl. ¶ 560), and may also use other social networks. California courts repeatedly have held that services of this sort do not implicate *Tunkl*. *See City of Santa Barbara v. Super. Ct.*, 41 Cal. 4th 747,

[1] Plaintiffs also do not dispute that the Communications Decency Act, 47 U.S.C. § 230, bars certain claims based on the acts of third parties on Facebook's platform. *See* MTD at 32 n.14.

757–58 (2007) (citing cases). Facebook's services "[are] not so essential as to rob [P]laintiff[s] of [their] free will in deciding" whether to consent to terms. *YMCA of Metro. L.A. v. Super. Ct.*, 55 Cal. App. 4th 22, 27 (1997); *Corby v. Kloster Cruise Ltd.*, 1990 WL 488464, at *3 (N.D. Cal. Oct. 5, 1990).

Plaintiffs' unconscionability arguments also fail as a matter of law. Their *only* argument for procedural unconscionability is that users "lack bargaining power" (Opp. at 19)—presumably on the premise that the SRR is an adhesion contract—but there is no rule in California "that an adhesion contract is per se unconscionable." *See Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1261 (9th Cir. 2017). And Plaintiffs' only argument for substantive unconscionability is that the waiver provision "is one-sided" (Opp. at 19), but that is also insufficient. Plaintiffs admit that the SRR granted them a number of broad rights, Compl. ¶¶ 216-240, and do not point to any terms that "shock the conscience" or were "overly harsh, unduly oppressive, [or] unreasonably favorable." *Poublon*, 846 F.3d at 1261 (citations omitted).

E. Facebook Did Not Violate The VPPA

Plaintiffs also offer nothing to save their VPPA claim. They make the obvious point that websites offering video streaming services can be "video tape service providers," but make no attempt to explain how Facebook meets this definition. *See* Opp. at 20. Unlike Hulu, a service devoted exclusively to video streaming, Facebook's services do not involve the rental or sale of videos. *See* S. Rep. No. 100-599, at 12 (1998) ("simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of the bill."). The VPPA does not apply to disclosures unrelated to these types of transactions. *See id.* at 12 ("a department store that sells video tapes would be required to extend privacy protection to only those transactions involving the purchase of video tapes and not other products"); *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1170 (W.D. Wash. 2010) ("Amazon may not disclose records regarding its customer's video or audiovisual purchases"). Put another way, Facebook's provision of social networking services allowing users to share videos does not make it a video tape service provider under the VPPA.

Plaintiffs also do not allege that Facebook disclosed personally identifiable information ("PII") within the VPPA's specific definition of that term: "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C.

§ 2710(a)(3). This definition "is intended to be transaction-oriented," limited to "information that identifies a particular person has having engaged in a specific transaction." S. Rep. No. 100-599 at 12 (1998). For example, the VPPA does not prohibit disclosure of a person's views about a film; it prohibits disclosure only of information showing that a person actually requested or obtained that film from an entity subject to the Act's regulation. Accordingly, virtually every VPPA case has involved the alleged disclosure of a record of a video transaction itself. *See, e.g.*, *Bernardino v. Barnes & Noble Booksellers, Inc.*, 2017 WL 3727230, at *3 (S.D.N.Y. Aug. 11, 2017); *Yeshov v. Gannet Satellite Info. Network, Inc.*, 204 F. Supp. 3d 353, 355 (D. Mass. 2016); *Perry v. Cable News Network, Inc.*, 854 F. 3d 1336, 1339 (11th Cir. 2017).

Plaintiffs allege no such disclosure here. They say that Facebook discloses various kinds of video-related information and content, but none of these alleged disclosures meets the VPPA's narrow definition of PII because they do not identify a user as having "*requested or obtained specific video materials or services from a video tape service provider*." A user's *own* videos on Facebook are not PII under the VPPA because the user does not request or obtain them from Facebook. Videos in which a user is tagged are not PII under the VPPA because a "tag" is a statement that the user is in the video, not that he or she has requested or obtained it. Indeed, tagging does not indicate any action by that user at all. A user's page "likes" are not PII under the VPPA because they merely indicate that a user has connected to a Facebook page (for a number of reasons), and they do not request or obtain any video that might be featured on the page. And videos in a user's News Feed are not PII under the VPPA because Facebook determines what content appears there, and the fact that a video was in a user's feed does not identify that user as having requested or even watched that video.

F. Plaintiffs have not alleged a violation of the Stored Communications Act

The Opposition offers no theory to support Plaintiffs' SCA claims, which must be dismissed.[2] By agreeing to Facebook's SRR and Data Use Policy, Plaintiffs consented to data sharing with third-party apps and the other entities alleged in the complaint. *See supra* pp. at 5-7. Although Plaintiffs claim that any consent would not apply to categories that "plaintiffs configured to be non-public" (Opp. at 23),

[2] Plaintiffs concede that they have no viable claim under 18 U.S.C. § 2701(a). Opp. at 22 n.19.

their own allegations defeat this theory by admitting that Facebook provides user data only "[a]s long as the request complies with the users' and/or friends' privacy settings." Compl. ¶¶ 121–22; *see Weisbuch v. Cty. of L.A.*, 119 F.3d 778, 783 n.1 (9th Cir. 1997) (claim subject to dismissal where plaintiffs have "ple[d] [themselves] out of court"). Indeed, not one of the 34 named plaintiffs alleges a single category of data they maintained on Facebook as non-public. MTD at 30; Opp. at 23–24 (listing several categories of Facebook user data). Plaintiffs' only response is that the Court should "infer[]" that all the Plaintiffs configured their settings to be non-public (Opp. at 23), but that gets pleading rules backward: Plaintiffs must plead actual facts showing their alleged injuries are covered by the SCA. *See Wasson v. Sonoma Cty. Jr. Coll. Dist.*, 4 F. Supp. 2d 893, 908 (N.D. Cal. 1997), *aff'd*, 203 F.3d 659 (9th Cir. 2000) (dismissing privacy claims where plaintiff "has not alleged what [Defendants] disclosed, if anything, that was not already disclosed to the public by [the plaintiff]").

Plaintiffs point to allegations that they used Facebook Messenger, arguing that such information is "by definition" non-public. Opp. at 23. But Plaintiffs do not allege that Kogan's app obtained any of their messages and, in fact, they admit that the app obtained messages from only 1,500 of the app's 300,000 downloading users (Compl. ¶ 139), making it extremely unlikely any named plaintiff's messages were obtained. Nor do Plaintiffs dispute that any consent given by those downloading users defeats their SCA claims because the SCA does not require consent from both the sender *and* recipient, but rather permits disclosure with "the lawful consent of the originator *or an addressee or intended recipient* of [the] communication, or the subscriber. 18 U.S.C. § 2702(b)(3) (emphasis added). Plaintiffs deny that these downloading users consented to obtain Facebook messages, but that denial is contradicted by the July 11, 2018 ICO Report on which Plaintiffs rely: the app "utilised the Facebook Login in order to *request permission from the app user*" to access a small number of users' "Facebook messages." ICO, *Investigation into the Use of Data Analytics in Political Campaigns – Investigation Update* 19-20 (July 11, 2018) (emphasis added), https://bit.ly/2KOJ67V; Compl. ¶¶ 145–149 & nn.22–27.

G. Plaintiffs Have Not Adequately Alleged Any Privacy Claims

1. ***Plaintiffs have not alleged a reasonable expectation of privacy because they have not specified what content they shared.*** Rather than identifying specific sensitive information that was disclosed, Plaintiffs suggest that alleged disclosures of general "categories" of "content and information" suffice.

Opp. at 24. But Plaintiffs' generalized allegations cannot establish the "dissemination or misuse of *sensitive* and *confidential* information," necessary to state a privacy claim. *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1039 (N.D. Cal. 2014) (quoting *Hill v. NCAA*, 7 Cal. 4th 1, 35 (1994)) (emphasis added). "[T]here is no legally protected privacy interest and reasonable expectation of privacy in" these categories of information "as a general matter." *See id.* at 1041. Rather, Plaintiffs must specifically allege that the disclosure "actually included content that qualifies under California law as 'confidential' or 'sensitive.'" *Id*. Merely alleging that generic types of content—like "photos" shared with any number of Facebook friends—may have been disclosed is insufficient to show that the photos were, in fact, so sensitive that there was "an egregious breach of the social norms underlying the privacy right." *Hill*, 7 Cal. 4th at 37.

Plaintiffs do not allege *any* specific facts regarding content they shared on Facebook that allegedly was disclosed or how that specific content was "sensitive." And they do not distinguish the cases dismissing privacy claims like those here where plaintiffs fail to specify exactly what *protected* information was disseminated. *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1035 (N.D. Cal. 2014) (holding that plaintiff cannot "claim a reasonable expectation of privacy with respect to his text messages, in general" and dismissing complaint where "[t]he pleadings do not identify the contents of any particular text messages, and instead, refer generally to 'private electronic data and electronic communications.'"); *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014); *Scott-Codiga v. Cty. of Monterey*, 2011 WL 4434812, at *7 (N.D. Cal. Sept. 23, 2011); *Wasson*, 4 F. Supp. 2d at 908.

In re Yahoo Mail Litigation is squarely on point. Just like the plaintiffs here, the plaintiffs in that case alleged that a generic category of content—their emails—was disclosed to third parties, without identifying any specific information the emails contained. Without such specifics, "Plaintiffs' claim fail[ed] as a matter of law" because there is no "legally protected privacy interest or reasonable expectation of privacy in email *generally*." 7 F. Supp. 3d at 1040. "Rather, the cases in which courts have found a protected privacy interest in the context of email communications have done so in circumstances where the plaintiff alleged *with specificity* the material in the content of the email." *Id*. at 1041. This rule makes perfect sense: "Even disclosure of very personal information has not been deemed an 'egregious breach of social norms' sufficient to establish a constitutional right to privacy," so courts must "make their decisions regarding whether a plaintiff has stated a legally protectable privacy interest based on the nature

of the information at issue." *Id*. at 1038, 1041. Here, as in *Yahoo*, Plaintiffs cannot do so merely by asserting that their content was "sensitive," as such allegations are "fatally conclusory." *Id*. at 1041.

2. ***Plaintiffs have not alleged "highly offensive" conduct that amounted to an "egregious breach of social norms."*** Plaintiffs' failure to identify any specific information that was shared also forecloses their argument that Facebook's conduct "would be 'highly offensive to a reasonable person.'" Opp. at 25. Plaintiffs offer no meaningful basis to evaluate the factors they argue inform that inquiry—"the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion," "the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded," *id.*—because they do not allege what specific content was disclosed. Plaintiffs' various arguments add nothing to the general, nonspecific and boilerplate assertions in the Complaint. They argue that "Facebook intruded upon a vast array of information regarding Plaintiffs," *id.*—but the Complaint contains not a single allegation about what specific information the named plaintiffs may have provided. They say that this "vast array" "includ[ed] personal and family photographs," *id.*—but no such allegation appears in the Complaint. They assert that Facebook "did so despite Plaintiffs' express designation of such information as non-public," *id.*—but they allege nothing about their privacy settings, and do not dispute that the thisisyourdigitallife app could obtain their information only if their privacy settings allowed it. They assert that "Facebook misrepresented its practices and policies regarding data sharing to Plaintiffs"—but do not address the clear and express language in the Data Use Policy stating that "if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use." Compl. ¶ 275. In the end, Plaintiffs cite no allegation to support the notion that they had "a reasonable expectation of privacy"—and there is none in the Complaint.

Nor do any of Plaintiffs' cases hold that generalized allegations are enough to plead "conduct that would be 'highly offensive to a reasonable person.'" Opp. at 25. In *Miller v. NBC*, 187 Cal. App. 3d. 1463 (1986), a film crew followed paramedics into a home without consent, filmed a man suffering a heart attack in his bedroom, and then ran the footage repeatedly on TV. *Id.* at 1469. The court found that the man's wife had a valid intrusion on seclusion claim because the film crew's conduct was contrary to "widely held notions of decency" and "most individuals understand that [such conduct] is a tort, a crime, or both." *Id.* at 1483. Thus, "reasonable people could regard the NBC camera crew's intrusion

into [the decedent's] bedroom at a time of vulnerability and confusion occasioned by his seizure as 'highly offensive' conduct." *Id.* at 1484. Needless to say, nothing remotely similar is alleged here.

In *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064 (N.D. Cal. 2016), the plaintiffs' intrusion claim was based on Yelp's allegedly improper downloading of their iPhone contacts—a practice it did not disclose in its privacy policy. *Id*. at 1074, 1077. Here, by contrast, Facebook's privacy policy is clear: "if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use." Compl. ¶ 275. The only conduct Plaintiffs allege affected them personally—the sharing of information with a single app—falls squarely within that disclosure.

Plaintiffs argue that Facebook's conduct was "'sufficiently serious' to constitute an 'egregious breach of social norms.'" Opp. at 26 (quoting *Hill*, 7 Cal.4th at 37). They cite *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015), a case about covert surveillance of individuals' Internet browsing via electronic cookies. The defendant in that case allegedly *overrode* plaintiffs' cookie blockers "while concurrently announcing in its Privacy Policy that internet users could 'reset [their] browser to refuse all cookies,'" and the Third Circuit held that this alleged "deceitful override" could have intruded on plaintiffs' reasonable expectations of privacy. *Id.* at 150, 151, 153. No such deceit is alleged here. Plaintiffs admit that Facebook provided users with tools to prevent sharing with apps, and do not allege any conduct that was inconsistent with Plaintiffs' actual settings. As Plaintiffs admit, apps, including thisisyourdigitallife, could obtain user data only "[a]s long as the request complie[d] with the user's and/or friends' privacy settings." Compl. ¶¶ 121–22, 138.

Nothing in *Goodman v. HTC America, Inc.* is to the contrary. *Goodman* recognized California law holding that collecting PII like "someone's address or telephone number" is "routine commercial behavior," not an egregious breach of social norms. 2012 WL 2412070, at *15. But the court found that "[c]ollection of fine location data is more sensitive than collecting home addresses or telephone numbers because people often carry their smartphones with them wherever they go." *Id*. "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id*. This is not a GPS monitoring case. And unlike the "wealth of detail" from alleged GPS tracking, the sensitivity of the information Plaintiffs claim was disclosed here depends on, among other things, what information they

chose to share. *See Yahoo*, 7 F. Supp. 3d at 1041.

3. ***Plaintiffs have not stated a claim for public disclosure of private facts.*** Plaintiffs' claim for public disclosure of private facts fails because Plaintiffs do not and cannot allege that any facts at issue were non-public or that any facts were publicly disclosed. Plaintiffs failed to allege that any disclosed information was private and they do not contest that "[a] matter that is already public or that has previously become part of the public domain is not private." *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1130 (2018). Their only response is to reference their SCA arguments where they ask the court to "infer" that they set their profiles to be non-public, Opp. at 23, but they offer no basis to make any such inference, as they do not allege that *any* named plaintiff set his or her privacy settings to non-public. Moreover, to plead a privacy claim, Plaintiffs must affirmatively allege that the disclosed information was not already public and that its specific content made its disclosure an egregious breach of social norms. *Wasson*, 4 F. Supp. 2d at 908. Plaintiffs did not do so here.

Nor can Plaintiffs allege the necessary element of public disclosure because disclosure to a single app developer is not "public" disclosure. Although Plaintiffs assert that "Facebook 'published private content and information of Plaintiffs and Class Members to … millions of app developers" (Compl. ¶ 522), the only app they identify as having accessed their information is thisisyourdigitallife. Plaintiffs cite a case holding that sending defamatory letters to 20 people in various states "adequately reflects 'mass exposure'" (Opp. at 27), but they do not cite any case holding that disclosure to a single entity is "mass exposure." And Plaintiffs' assertion that "Facebook published this information to other third parties" (*id.*) is unsupported by any specific allegation in the Complaint. Indeed, the Complaint makes clear that *Facebook* did not actually disclose user data: the downloading user granted Kogan permissions to access his or his friends' data, and Facebook provided that data only pursuant to those permissions "as long as the request complies with the user's and/or friends' privacy settings." Compl. ¶¶ 121–22.

4. ***Plaintiffs have not stated a claim for violation of their right to publicity.*** Plaintiffs' Opposition confirms that they have no right of publicity claim. Their theory appears to be that providing users' PII to advertisers amounts to an "appropriation of their name and likeness," without regard to whether the advertiser publicly traded on that likeness when advertising its products. Opp. at 27-28. But this argument goes nowhere. Even apart from the dispositive consent issues noted above, and the fact that

the Complaint contains no allegation that Facebook shares individual user data with advertisers, "[d]emographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers," *Goodman*, 2012 WL 2412070, at *7, and collecting such information has never been deemed to constitute a violation of the right to publicity—or even implicate publicity at all.

Plaintiffs point out that "California law … protects non-celebrity plaintiffs from the appropriation of their name and likeness." Opp. at 27. But that truism does not address the basic flaw in their claim: they have not alleged that anyone "merchandis[ed]" their likeness by, for example, publicly associating it with a product without consent. *See Timed Out, LLC v. Youabian, Inc.*, 229 Cal. App. 4th 1001, 1006 (2014). In all of Plaintiffs' cases, the right of publicity protected individuals' ability to control the *public* commercialization of their likeness. *See id.* at 1013 (Defendants "use[d] … the Models' likenesses pictured in the photographs to promote [their] business"); *Eastwood v. Sup. Ct.*, 149 Cal. App. 3d 409 (1983) (defendants used celebrity's "personality and fame" for commercial advantage); *KNB Enters. v. Matthews*, 78 Cal. App. 4th 362, 364 (2000) (appropriation of the models' photographs through unauthorized commercial display on defendant's website); *Dora v. Frontline Video, Inc.*, 15 Cal. App. 4th 536, 540 (1993) (unauthorized use of surfer's voice and image in documentary). Plaintiffs make no similar allegation in this case of any commercial use of their names or likenesses.

H. Plaintiffs Have Not Stated A Claim For Fraudulent Omission

Plaintiffs also fail to state a claim for fraudulent omission. They contend that Facebook "failed to disclose the known risk that third-party app developers would sell or disperse user content and information." Opp. at 29. But they acknowledge (Compl. ¶¶ 560–561) that Facebook's Data Use Policy told users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook." Duffey Decl. Ex. 45 at 9. Likewise, the SRR stated that a user's "agreement with [an] application will control how the application can use, store, and transfer … content and information," *id.*, Ex. 21 at 1 (Oct. 4, 2010 SRR); Compl. ¶¶ 221–222, and contained a broad waiver of liability for claims based on third-party conduct, Duffey Decl. Ex. 21 at 3. These statements sufficiently informed users about the potential risks associated with third-party apps.

Plaintiffs' only response is that this is a question of fact, cross-referencing Section II.B.3 of their brief. Opp. at 29. But that section does not discuss the sufficiency of the disclosures relevant to their

concealment theory or any other elements of an omission claim. In fact, courts routinely resolve fraud claims on the pleadings where the allegedly concealed information was disclosed or was publicly available. *See Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1163–64 (9th Cir. 2012) (no concealment claim where plaintiff "was able to discover the annual fee" by "scroll[ing] through the" terms on a website); *Porras v. StubHub, Inc.*, 2012 WL 3835073, at *5 (N.D. Cal. Sept. 4, 2012) (no UCL fraud claim); *Meyer v. Aabaco Small Bus., LLC*, 2018 WL 306688, at *3–5 (N.D. Cal. Jan. 5, 2018) (same).

Plaintiffs' attempt to ground a disclosure duty on statements by Facebook's executives (Opp. at 29) fails because no plaintiff alleges awareness of those statements or reliance on them to their detriment.

Plaintiffs next argue that Facebook "concealed that it distributes users' content and information to app developers, as well as its 'business partners.'" Opp. at 29. But Plaintiffs do not even address Facebook's arguments on this point. MTD at 35-36. Plaintiffs' only retort is that Facebook has "identifie[d] no disclosures at all about giving business partners such as mobile carriers and chip designers access to Plaintiffs' content and information." Opp. at 30. That is incorrect. The Data Use Policy stated plainly, "[w]e give your information to the people and companies that help us provide the services we offer." *See, e.g.*, Compl. ¶¶ 281–84. And Plaintiffs' failure to allege that they personally were harmed by alleged disclosures to unknown "business partners" makes their assertion about Facebook's disclosures regarding business partners irrelevant.

Plaintiffs' next theory is that Facebook failed to "disclose … how [its] content and information was being collected, shared and aggregated to develop digital dossiers of each user." Compl. ¶ 503. Plaintiffs do not dispute that Facebook disclosed that it earns revenue through targeted advertising, and concede that Cambridge Analytica purchased data from *Kogan*, not Facebook, Compl. ¶ 142. Their only argument is that Facebook should have told them that it enables so-called "psychographic advertising" and that it targeted them by "individual demographic traits," Opp. at 30, but they cite no authority requiring these kind of minutely detailed "disclosures" about Facebook's business. In any event, the Data Use Policy disclosed that Facebook "may also put together data about you to serve you ads that might be more relevant to you." *E.g.*, Duffey Decl., Ex. 45 at 4 (Dec. 11, 2012 Data Use Policy).

Nor do Plaintiffs explain how they were harmed by any targeted advertising, or how knowing more about Facebook's advertising practices would have caused them to act differently. They argue only

that "actions that a plaintiff undertakes—but would not have undertaken had the defendant told the truth—are compensable." Opp. at 30. But it is *injuries* that are compensable, and there must be some logical connection between the alleged injury and the conduct challenged. *Tenet Healthsystem Desert, Inc. v. Blue Cross of California*, 245 Cal. App. 4th 821 (2016), illustrates the point. There, an insurer allegedly concealed that a patient's policy excluded him from coverage, causing the hospital reasonably to "believe that the services would be paid for." *Id*. at 845. There was a causal link between the hospital's harm—the unreimbursed treatment expenses—and the insurer's alleged fraud. *Id*. at 844–45. Here, Plaintiffs have not attempted to draw a link between their concealment theories and any alleged harm.

Plaintiffs cite *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015), which involved software that surreptitiously tracked users' browsing activities. Unlike here, there was no question that the alleged conduct was not disclosed, and there was a clear causal link between the alleged harm and the concealment: The plaintiffs plausibly alleged that they would have purchased different phones if they had known. *Id*. at 1113. Here, all of the allegedly concealed information was disclosed, and the purported omissions largely concern practices that Plaintiffs do not allege harmed them personally.

I. Plaintiffs' UCL Claims Fail

Plaintiffs' UCL claims fail because they lack standing and have not alleged a UCL violation.

1. ***Plaintiffs lack statutory standing.*** To bring a UCL claim, Plaintiffs must "ha[ve] suffered injury in fact and ha[ve] lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *Kwikset Corp. v. Sup. Ct.*, 51 Cal. 4th 310, 320–21 (2011). Plaintiffs offer no theory of economic loss caused by Facebook's conduct. MTD at 43. Instead, they argue that they "conveyed their personal content and information to Facebook, that this content and information is of value, and that Facebook has wrongfully … profited from" it. Opp. at 31. But, as Facebook showed, a defendant's profit from information does not equate to economic *loss*. MTD at 43. In any event, Facebook does not generate revenue from app developers (and Cambridge Analytica did not pay Facebook for the data it obtained from Kogan; the money was paid to Kogan, Compl. ¶ 142). Rather, its revenue comes largely from ads, *id.* ¶ 359, and Plaintiffs do not allege that Facebook gives individual user data to advertisers.

Nor can Plaintiffs offer any cognizable right to restitution, which is their only theory in response to this point. Opp. at 32. Plaintiffs articulate two restitution theories to try to avoid the fact that Facebook

is a free service, thus precluding any possible restitution claim: (1) credit-monitoring expenses and (2) "Facebook's exploitation of Plaintiffs' property interest in their content and information." *Id*. Both fail because "[a] restitution order … requires both that money or property have been lost by a plaintiff … , and that it have been acquired by a defendant." *See Kwikset*, 51 Cal. 4th at 336. Facebook did not receive any benefit as a result of Plaintiffs' allegedly seeking identity theft monitoring services. *See Ruiz v. Gap, Inc.*, 2009 WL 250481, at *4 (N.D. Cal. Feb. 3, 2009), *aff'd*, 380 F. App'x 689 (9th Cir. 2010). And Plaintiffs cannot allege that they lost any money or property by giving Facebook their user data. "'[P]ersonal information' does not constitute money or property under the UCL." *iPhone Application Litig.*, 2011 WL 4403963, at *14; *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *4 (N.D. Cal. Mar. 26, 2013); *Facebook Privacy Litig.*, 791 F. Supp. 2d at 714–15.

At bottom, Plaintiffs do not seek restitution in the proper sense of the word. Restitution seeks to restore the status quo by returning to the plaintiff funds he or she owned. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1149 (2003). Here, as in *Korea Supply*, Plaintiffs cannot seek restitution because Facebook is a free service and Plaintiffs lack any ownership interest in Facebook's alleged profits. *See Cortez v. Purolator Air Filtration Prods. Co.*, 23 Cal. 4th 163, 177 (2000) ("The status quo ante to be achieved by the restitution order" is to restore money that "had been in the [victim's] possession.").

2. ***Facebook's conduct was not unfair, fraudulent, or unlawful.*** Plaintiffs also cannot state a substantive claim under the UCL. They offer a hodgepodge of public policy theories to support their claim of "unfair" conduct, but a plaintiff alleging "unfair" conduct under the UCL "must show the conduct 'threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws." *Byars v. SCME Mortg. Bankers, Inc.*, 109 Cal. App. 4th 1134, 1147 (2003) (quoting *Cel-Tech Commc'n, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 187 (1999)). Plaintiffs' contention that this definition does not apply in consumer cases (Opp. at 32 n. 24) is incorrect, as *Byars* was a consumer case.

Plaintiffs' claim of "unlawful" conduct under the UCL rests solely on their VPPA and SCA claims, Opp. at 31, and fails for the same reasons as do those claims. Finally, Plaintiffs' claim of "fraudulent" conduct rests solely on their fraudulent omission claim, and, again, fails for the same reasons.

J. Plaintiffs Cannot Bring A Standalone Unjust Enrichment Claim

"Unjust enrichment is not a cause of action, just a restitution claim." *Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307 (2011). Thus, an "unjust enrichment claim does not properly state an independent cause of action," *Low*, 900 F. Supp. 2d at 1031, and should be "construe[d] … as a quasi-contract claim seeking restitution." *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015). Plaintiffs cannot state any claim for restitution, and, in any event, California law does not allow quasi-contract claims where there is "a valid express contract covering the same subject matter." *Cheung v. Wells Fargo Bank, N.A.*, 987 F. Supp. 2d 972, 979 (N.D. Cal. 2013); *Zepeda v. PayPal, Inc.*, 777 F. Supp. 2d 1215, 1223 (N.D. Cal. 2011). Plaintiffs' reliance on *Moeller v. American Media, Inc.*, 235 F. Supp. 3d 868 (E.D. Mich. 2017), is unavailing because, in that case, there was no valid express contract.

Plaintiffs argue it is premature to dismiss the unjust enrichment claim, but as these cases attest, courts routinely dispose of such claims where the plaintiff pleads breach of a written contract covering the same subject matter as the quasi-contract claim. Plaintiffs also argue that the Court should not dismiss their unjust enrichment claim because Facebook's purported "sale of user data to third-party business partners was not covered by the SRR." Opp. at 34. But, as shown above, the conduct that Plaintiffs incorrectly describe as "selling" user data is plainly covered by the Data Use Policy, which was incorporated into the SRR, and thus formed a part of the contract under which Plaintiffs seek to recover.

K. Plaintiffs' Negligence Claims Fail

Plaintiffs' negligence claims fail for several reasons. First, Plaintiffs do not address Facebook's point that their theory of duty—that Facebook allegedly had a duty to ensure that no third parties "were improperly collecting, storing, obtaining and/or selling" content and information (Compl. ¶ 547)—falls squarely within the SRR's specific limitation of liability. *See supra* pp. 10-11.

Second, Plaintiffs do not deny the "general rule" that "one owes no duty to control the conduct of another, nor to warn those endangered by such conduct" (*Davidson v. City of Westminster*, 32 Cal. 3d 197, 203 (1982); *see also* Rest. (Second) of Torts §§ 314, 315)—the very duty Plaintiffs seek to impose.

Third, the absence of a "special relationship" between Plaintiffs and Facebook bars tort claims. Courts look to six factors: (1) whether the transaction was intended to affect the plaintiff, (2) the foreseeability of harm, (3) the degree of certainty of harm, (4) the connection between the conduct and the harm,

(5) the moral blame attached to the conduct and (6) the policy of preventing future harm. *J'Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979). Every factor refutes the existence of a special relationship here.

Plaintiffs do not address Facebook's argument that the first *J'Aire* factor applies *only* when conduct is unique to them, as opposed to all users. *See Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1230–31 (2008). When the "sales at issue [a]re like any other … sale" by the defendant, the first factor is not met. *Id.* at 1231; *Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1054 (N.D. Cal. 2004). Plaintiffs do not allege that Facebook intended to affect them specifically.

For the second and third factors, Plaintiffs allege no cognizable harm, thus mooting any analysis of foreseeability or certainty. *Cf. J'Aire*, 24 Cal. 3d at 805 (third factor met when complaint leaves "no doubt" of harm). As to factor four, the connection between Facebook's actions and Plaintiffs' alleged injuries is tenuous at best. Plaintiffs concede that any alleged misuse of data was by app developers, not Facebook, Opp. at 37, but fail to acknowledge that Facebook required app developers to agree to policies forbidding the sale of user data. Because there is no close connection between Facebook's actions and Plaintiffs' alleged injuries, Plaintiffs' arguments concerning moral blame (factor five) also fail. And there is little risk of future harm (factor six) because Facebook changed the Graph API in 2015 to allow apps to access data only from the people who authorize the app.

The cases that Plaintiffs cite do not help them. In *In re Yahoo! Inc. Consumer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113 (N.D. Cal. 2018), Yahoo! repeatedly failed to institute adequate security measures, with the result that hackers obtained users' sensitive financial and medical data and plaintiffs suffered concrete harms such as tax fraud and theft of Social Security benefits. *Id.* at 1124, 1132. Here, by contrast, Plaintiffs concede that the thisisyourdigitallife app could obtain their information only if their settings allowed it, rendering inapposite the *Yahoo!* court's conclusions about foreseeability and morality.

L. Plaintiffs Have Not Adequately Alleged A Breach Of Contract

Plaintiffs point to no contractual provision that Facebook allegedly breached. They claim that Facebook breached its commitment not to "share [users'] content and information with advertisers without your consent." Opp. at 39. But the Data Use Policy clearly disclosed that people could share friends' information with third parties, and that Facebook shared information with service providers. Plaintiffs

also contend that Facebook "breached the SRR provision that users owned all of the content and information they posted on Facebook and could control how it is shared." *Id*. at 40. But Plaintiffs acknowledge that they *could* control how their information was shared, *id*. at 17, as described in the Data Use Policy. Plaintiffs do not claim that they were unable to turn off app sharing entirely, only that it was inconvenient. And Plaintiffs still offer no cognizable theory of injury, which, by itself, is sufficient to defeat their contract claims. *See supra* pp. 2-5.

Finally, Plaintiffs cannot rely on the implied covenant of good faith and fair dealing. Opp. at 41. The very actions Plaintiffs say violated the implied covenant—sharing "content and information" with advertisers, providing data to certain third parties, and allowing users "to be targeted by" ads—all were expressly covered by the Data Use Policy, which was itself part of Facebook's contract with users.

M. Many Of Plaintiffs' Claims Are Barred By The Statute Of Limitations

Plaintiffs argue that the 2015 *Guardian* article about Cambridge Analytica's improper acquisition of Facebook user data did not start the limitations period for their claims because it focused on Cambridge Analytica, not Facebook. Opp. at 41–43. But that article provided all of the key information underlying Plaintiffs' allegations that Facebook did not do enough to protect user data. It stated that Cambridge Analytica improperly obtained the data of "tens of millions of Facebook users, harvested largely without their permission," including "names, locations, birthdays, genders—as well as . . . Facebook 'likes.'" Indeed, the article's title alone—"Ted Cruz using firm that harvested data on millions of unwitting Facebook users"—should have alerted Plaintiffs that Cambridge Analytica had accessed user data. Courts impute knowledge to plaintiffs where, as here, there is widespread publicity. *See United Klans of Am. v. McGovern*, 621 F.2d 152, 154 (5th Cir. 1980) (knowledge imputed where three major networks reported on issue); *Stutz Motor Car of Am., Inc. v. Reebok Int'l, Ltd.*, 909 F. Supp. 1353, 1362 (C.D. Cal. 1995) (similar); *McKelvery v. Boeing N. Am., Inc.*, 74 Cal. App. 4th 151, 159–60 (1999) (similar). By December 2015, the wide reporting here gave Plaintiffs "a reason at least to suspect a factual basis for [the] elements" of their claims, barring all of their claims with a two-year statute of limitations. *Fox v. Ethicon Endosurgery, Inc.*, 35 Cal. 4th 797, 807 (2005).

Plaintiffs nevertheless claim that they could not discover an alleged injury because Facebook did not notify users whose data may have been obtained. *See* Opp. at 43. But the whole point of constructive

notice by widespread publication is that it serves the same function as direct notification. And, in any event, at least 15 plaintiffs in this MDL determined that Cambridge Analytica might have obtained their data *before* Facebook began notifying affected users on April 9, 2018, as they filed suit before that date.[3]

N. Plaintiffs' Non-California Claims Should Be Dismissed With Prejudice

Because Plaintiffs concede that California law governs (Compl. ¶¶ 19–20), there is no reason to delay dismissing with prejudice Plaintiffs' 31 "non-priority" non-California causes of action. Plaintiffs do not dispute that these claims are not viable. Yet they suggest that dismissal should be granted without prejudice or denied outright because Pretrial Order No. 12 stayed non-priority claims. Opp. at 43. Plaintiffs offer no reason to delay resolving these claims, which present a straightforward choice-of-law issue, the resolution of which would greatly simplify this case. *See* MTD at 44–45.

O. Leave To Amend Should Be Denied

Courts should not allow amendment under Rule 15 where, as here, the proposed amendment would be futile. *Foman v. Davis*, 371 U.S. 178, 182 (1962); *Johnson Mammoth Recreations, Inc.*, 975 F.2d 604, 607 (9th Cir. 1992). Plaintiffs speculate that ongoing investigations and recent articles will supply them with facts to establish standing (Opp. at 44; Weaver Decl. Exs. 3–4), but they cannot keep this case alive to wait and see if some future development provides a cause of action. *See Operational Risk Mgmt. LLC v. Union Bank, N.A.*, 2012 WL 1710893, at *3 (N.D. Cal. 2012). Nor is additional information *about the named plaintiffs* likely to emerge that would show standing. Plaintiffs already filed dozens of complaints, received discovery, and engaged in multiple colloquies with this Court about the flaws in their complaints before drafting the Consolidated Complaint. Yet Plaintiffs *still* do not allege any injury-in-fact. Because the facts are in Plaintiffs' own possession, leave to amend is unwarranted. *See Sebastian Brown Prods. LLC v. Muzooka Inc.*, 2016 WL 949004, at *16 (N.D. Cal. Mar. 14, 2016).

III. CONCLUSION

This Court should dismiss Plaintiffs' Consolidated Complaint without leave to amend.

---

[3] Plaintiffs reliance on other statements does not help them. They argue that, *4 years before* the *Guardian* article, Facebook entered into an FTC consent decree and that an auditor later certified its compliance. *See* Opp. at 42. But these non-public, third-party reports did not "conceal" information. Plaintiffs also point to statements Facebook made in 2018 about Cambridge Analytica, but those statements were not misleading and, as explained above, the statute of limitations already had run.

DATE: December 21, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER, LLP

By: */s/ Orin Snyder*

Orin Snyder (*pro hac vice pending*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc.